

10/18/00

10-20-00

jc913 U.S. PTO
09/692/47
10/18/00

UTILITY PATENT APPLICATION TRANSMITTAL
(Only for new nonprovisional applications under 37 CFR 1.53(b))

Docket No. : 39478/RRT/S850
Inventor(s) : Craig L. Ogg and Piers C. Lingle
Title : MACHINE DEPENDENT LOGIN FOR ON-LINE VALUE-BEARING
ITEM SYSTEM
Express Mail Label No. : EL521375206US

ADDRESS TO: Assistant Commissioner for Patents
Box Patent Application
Washington, D.C. 20231

Date: October 18, 2000

1. ☒ **FEE TRANSMITTAL FORM** (Submit an original, and a duplicate for fee processing).

2. **IF A CONTINUING APPLICATION**

___ This application is a of patent application No. .

Prior application information: Examiner ; Group Art Unit:

☒ This application claims priority pursuant to 35 U.S.C. §119(e) and 37 CFR §1.78(a)(4), to provisional Application Nos. 60/160,040, 60/160,038, 60/160,491, and 60/160,708.

3. **APPLICATION COMPRISED OF**

Specification

41 Specification, claims and Abstract (total pages)

Drawings

17 Sheets of drawing(s) (FIGS. 1 to 9)

Declaration and Power of Attorney

___ Newly executed

☒ Unexecuted declaration

___ Copy from a prior application (37 CFR 1.63(d))(for continuation and divisional)

4. ___ **Microfiche Computer Program** (Appendix)

5. ___ **Nucleotide and/or Amino Acid Sequence Submission** (if applicable, all necessary)

___ Computer Readable Copy

___ Paper Copy (identical to computer copy)

___ Statement verifying identity of above copies

6. **ALSO ENCLOSED ARE**

___ Preliminary Amendment

___ A Petition for Extension of Time for the parent application and the required fee are enclosed as separate papers

___ Small Entity Statement(s)

___ Statement filed in parent application, status still proper and desired

UTILITY PATENT APPLICATION TRANSMITTAL
(Only for new nonprovisional applications under 37 CFR 1.53(b))

Docket No.: 39478/RRT/S850

- ☐ Copy of Statement filed in provisional application, status still proper and desired
- ☐ An Assignment of the invention with the Recordation Cover Sheet and the recordation fee are enclosed as separate papers
- ☐ This application is owned by pursuant to an Assignment recorded at Reel , Frame
- ☐ Information Disclosure Statement (IDS)/PTO-1449
- ☐ Copies of IDS Citations
- ☐ Certified copy of Priority Document(s) (*if foreign priority is claimed*)
- ☐ English Translation Document (*if applicable*)
- ☒ Return Receipt Postcard (MPEP 503) (should be specifically itemized).
- ☐ Other

7. CORRESPONDENCE ADDRESS

CHRISTIE, PARKER & HALE, LLP, P.O. BOX 7068, PASADENA, CA 91109-7068
CUSTOMER NUMBER: 23363

Respectfully submitted,

CHRISTIE, PARKER & HALE, LLP

By



Raymond R. Tabandeh
Reg. No. 43,945
626/795-9900

RRT/dsz

**FEE TRANSMITTAL
UTILITY PATENT APPLICATION**

DC913 U.S. PRO
09/692747
10/18/00

DATE: October 18, 2000

Docket No. : 39478/RRT/S850
Inventor(s) : Craig L. Ogg and Piers C. Lingle
Title : MACHINE DEPENDENT LOGIN FOR ON-LINE VALUE-BEARING ITEM
SYSTEM

FEE DETERMINATION

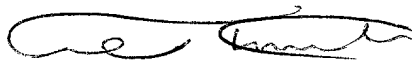
CLAIMS AS FILED					
	NUMBER FILED	NUMBER EXTRA	SMALL ENTITY RATE	LARGE ENTITY RATE	FEE
TOTAL CLAIMS	45 - 20	25	x \$9.00	25 x \$18.00	\$450.00
INDEPENDENT CLAIMS	4 - 3	1	x \$40.00	1 x \$80.00	\$80.00
MULTIPLE-DEPENDENT CLAIMS FEE			\$135.00	\$270.00	\$0.00
BASIC FEE			\$355.00	\$710.00	\$710.00
TOTAL FILING FEE					\$1,240.00
List Independent Claims: 1, 16, 29, 37					

METHOD OF PAYMENT

- ☒ No filing fee enclosed
- ☒ No Deposit Account Authorization.

Respectfully submitted,

CHRISTIE, PARKER & HALE, LLP

By 

Raymond R. Tabandeh
Reg. No. 43,945
626/795-9900

RRT/dsz
DSZ PAS280585.1*-10/18/00 3.02 PM

1 39478/RRT/S850

MACHINE DEPENDENT LOGIN FOR ON-LINE
VALUE-BEARING ITEM SYSTEM

5

CROSS-REFERENCE TO RELATED APPLICATIONS

This patent application claims the benefit of the filing date of United States Provisional Patent Applications Serial Nos. 60/160,040, filed October 18, 1999 and entitled "MACHINE
10 DEPENDENT LOGIN FOR ON-LINE POSTAGE SYSTEM"; and 60/160,038, filed October 18, 1999 and entitled "METHOD AND APPARATUS FOR DIGITALLY SIGNING AN ADVERTISEMENT AREA ON VALUE BEARING ITEMS," and 60/160,491, filed October 20, 1999 and entitled "SECURE AND RECOVERABLE DATABASE FOR ON-LINE POSTAGE SYSTEM"; and 60/160,708,
15 filed October 20, 1999 and entitled "MACHINE DEPENDENT LOGIN FOR ON-LINE POSTAGE SYSTEM"; the entire contents of which are hereby expressly incorporated by reference.

FIELD OF THE INVENTION

20

The present invention relates to secure printing of value-bearing items (VBI) preferably, such as postage, tickets, and coupons. More specifically, the invention relates to a graphical user interface (GUI) for logging into the system, recovering a password, and printing of VBI in a computer network environment.

25

BACKGROUND OF THE INVENTION

A considerable percentage of the United States Postal Service (USPS) revenue is from metered postage. Metered postage is generated by utilizing postage meters that print a special
30 mark, also known as postal indicia, on mail pieces. Generally, printing postage and any VBI can be carried out by using mechanical meters or computer-based systems.

With respect to computer-based postage processing systems, the USPS under the Information-Based Indicia Program (IBIP) has
35 published specifications for IBIP postage meters that identify

1 39478/RRT/S850

a special purpose hardware device, known as a Postal Security Device (PSD) that is generally located at a user's site. The
5 PSD, in conjunction with the user's personal computer and printer, functions as the IBIP postage meter. The USPS has published a number of documents describing the PSD specifications, the indicia specifications and other related and relevant information. There are also security standards for
10 printing other types of VBIs, such as coupons, tickets, gift certificates, currency, voucher and the like.

A significant drawback of existing hardware-based systems is that a new PSD must be locally provided to each new user, which involves significant cost. Furthermore, if the additional
15 PSD breaks down, service calls must be made to the user location. In light of the drawbacks in hardware-based postage metering systems, a software-based system has been developed that does not require specialized hardware for each user. The software-based system meets the IBIP specifications for a PSD, using a
20 centralized server-based implementation of PSDs utilizing one or more cryptographic modules. The system also includes a database for all users' information. The software-based system, however, has brought about new challenges.

The system should also be able to handle minor and
25 catastrophic database failures without impacting the integrity of the on-line VBI system and provide for recovery of the database to minimize or eliminate the loss of data. In a hardware-based system, security is generally handled by the local hardware piece, that is unique to each user and includes a
30 cryptographic module that encrypts that user's information. System recovery can generally be handled by replacing the corrupted local hardware pieces for each user that stores that user's information, however, data specific to that user may be lost. Nevertheless, for a software-based system, the system need

35

to be configured to handle such database failures without sacrificing a major data loss and system security.

5 Therefore, there is a need for a new method and apparatus for implementation of VBI printing via a user friendly GUI with a variety of selectable options.

SUMMARY OF THE INVENTION

10 In accordance with one aspect of the present invention, an on-line VBI printing system that includes one or more cryptographic modules and a database has been designed. The cryptographic modules serve the function of the PSDs and are capable of implementing a variety of required security standards.
 15 A client system provides a user friendly GUI for facilitating the interface of the user to the system. The GUI system includes wizards that help the user step-by-step with processes of registration, logging into the system, password recovery, and printing a VBI.

20 In one embodiment, the invention discloses an on-line system for providing an early warning to a user that has changed his/her computer (machine). The invention protects the user against someone else using the user's information and logging into the system on a different computer. In one aspect, the invention
 25 describes an on-line system for printing a value bearing item (VBI) comprising: a user using one or more computers connected to a computer network; a secret key for identifying a first computer used by the user for registering with the on-line system; a server system capable of communicating with the one or
 30 more user computers over the computer network for receiving user information and the secret key from the first computer and registering a user; and a re-registration wizard for requiring the user to re-register if a second computer used by the user is not the same as the first computer used for registering the user.

In another aspect, the invention describes an on-line system for printing a value bearing item (VBI) comprising: a user using one or more computers connected to a computer network; a memory for storing information specific to a first computer used by the user for registering with the on-line system, wherein the information is used by the server system to identify the first computer; a server system capable of communicating with the one or more user computers over the computer network for receiving user information and the computer information from the first computer; and a re-registration wizard for requiring the user to re-register if a second computer used by the user is not the same as the first computer used for registering the user. The information specific to the user computer include one or more of register settings, a processor's ID, machine configuration, a network card ID, and a user's private key.

It is to be understood that the present invention is useful for printing not only postage, but any value bearing items, such as coupons, tickets, gift certificates, currency, voucher and the like.

BRIEF DESCRIPTION OF THE DRAWINGS

The objects, advantages and features of this invention will become more apparent from a consideration of the following detailed description and the drawings, in which:

FIG. 1 is a block diagram for the client/server architecture according to one embodiment of the present invention;

FIG. 2 is a block diagram of a remote user computer connected to a server via Internet according to one embodiment of the present invention;;

FIG. 3 is a block diagram of servers, databases, and services provided by according to one embodiment of the present invention;

1 39478/RRT/S850

FIG. 4 is an exemplary process flow diagram for a Re-registration wizard;

5 FIGs. 5A-5J are exemplary screens for a registration process according to one embodiment of the present invention;

FIGs. 6A-6C are exemplary flow process diagrams for password recovery according to some embodiments of the present invention;

10 FIGs. 7A-7G are exemplary screens for supplying a secret code and password recovery according to one embodiment of the present invention;

FIGs 8A-8C are exemplary screens for password recovery according to one embodiment of the present invention; and

15 FIG. 9 is an exemplary screen for displaying a logo or slogan of an OEM or advertiser according to one embodiment of the present invention.

DETAILED DESCRIPTION

20 In one aspect, the system and method of the present invention prevent unauthorized electronic access to a database subsystem and secure customers' related data, among others. One level of security is achieved by protecting the database subsystem by a postal server subsystem. The postal server subsystem controls preferably, all communications with the
25 database subsystem by executing an authentication algorithm to prevent unauthorized access.

Another level of security is achieved by encrypting preferably, all communications between the client system and the postal server subsystem. The encryption-decryption function is
30 employed using commonly known algorithms, such as, Rivest, Shamir and Adleman ("RSA") public key encryption, DES, Triple-DES, Pseudo-random number generation, and the like algorithms. Additionally, DSA signature, and SHA-1 hashing algorithms may be used to digitally sign a postage indicium. Another level of
35 security is provided when a user attempts to launch the client

1 39478/RRT/S850

software from a different computer. In such a case, the client software detects that an encrypted user key that is stored on the user's machine is missing, and starts the re-registration process.

An exemplary on-line postage system is described in U.S. patent Application No. 09/163,993 filed September 15, 1998, the entire contents of which are hereby incorporated by reference herein. The on-line postage system includes an e protocol that operates in conjunction with the USPS requirements. The system utilizes on-line postage system software comprising user code that resides on a client system and controller code that resides on a server system. The on-line postage system allows a user to print a postal indicium at home, at the office, or any other desired place in a secure, convenient, inexpensive and fraud-free manner. The system comprises a user system electronically connected to a server system, which in turn is connected to a USPS system.

Each of the cryptographic modules may be available for use by any user. When a user requests a PSD service, one of the available modules is loaded with data belonging to the user's account and the transaction is performed. When a module is loaded with a user's data ,that module becomes the user's PSD. The database record containing each user's PSD data is referred to as the "PSD package" (security device transaction data). After each PSD transaction is completed, the user's PSD package is updated and returned to a database external to the module. The database becomes an extension of the module's memory and stores not only the items specified by the IBIP for storage inside the PSD, but also the user's personal cryptographic keys and other security relevant data items (SRDI) and status information needed for continuous operation. Movement of this sensitive data between the modules and the database is secured to ensure that PSD packages could not be compromised.

In one embodiment, the server system is remotely located in a separate location from the client system. All communications
 5 between the client and the server are preferably accomplished via the Internet. FIG. 1 illustrates a remote client system 220a connected to a server system 102 via the Internet 221. The client system includes a processor unit 223, a monitor 230, printer port 106, a mouse 225, a printer 235, and a keyboard 224.
 10 Server system 102 includes Postage servers 109, Database 130, and cryptographic modules 110.

An increase in the number of servers within the server system 102 will not negatively impact the performance of the system, since the system design allows for scalability. The
 15 Server system 102 is designed in such a way that all of the business transactions are processed in the servers and not in the database. By locating the transaction processing in the servers, increases in the number of transactions can be easily handled by adding additional servers. Also, each transaction processed in
 20 the servers is stateless, meaning the application does not remember the specific hardware device the last transaction utilized. Because of this stateless transaction design, multiple servers can be added to each appropriate subsystem in order to handle increased loads.

Furthermore, each cryptographic module is a stateless device, meaning that a PSD package can be passed to any device because the application does not rely upon any information about what occurred with the previous PSD package. Therefore, multiple
 25 cryptographic modules can also be added to each appropriate subsystem in order to handle increased loads. A PSD package for
 30 each cryptographic module is a database record, stored in the server database, that includes information pertaining to one customer's service that would normally be protected inside a cryptographic module. The PSD package includes all data needed
 35 to restore the PSD to its last known state when it is next loaded

1 39478/RRT/S850

into a cryptographic module. This includes the items that the
IBIP specifications require to be stored inside the PSD,
5 information required to return the PSD to a valid state when the
record is reloaded from the database, and data needed for record
security and administrative purposes.

In one embodiment, the items included in a PSD package
include ascending and descending registers (the ascending
10 register "AR" records the amount of postage that is dispensed or
printed on each transaction and the descending register "DR"
records the value or amount of postage that may be dispensed and
decreases from an original or charged amount as postage is
printed.), device ID, indicia key certificate serial number,
15 licensing ZIP code, key token for the indicia signing key, the
user secrets, key for encrypting user secrets, data and time of
last transaction, the last challenge received from the client,
the operational state of the PSD, expiration dates for keys, the
passphrase repetition list and the like.

As a result, the need for specific PSDs being attached to
specific cryptographic modules is eliminated. A Postal Server
subsystem provides cryptographic module management services that
allow multiple cryptographic modules to exist and function on one
server, so additional cryptographic modules can easily be
20 installed on a server.

Referring back to FIG. 1, Postage servers 109 include one
or more Postal servers and provide indicia creation, account
maintenance, and revenue protection functionality for the
exemplary on-line postage system. The Postage servers 109 may
30 include several physical servers in several distinct logical
groupings, or services as described below. The individual
servers could be located within one facility, or in several
facilities, physically separated by great distance but connected
by secure communication links.

35

Cryptographic modules 110 are responsible for creating PSDs and manipulating PSD data to protect sensitive information from disclosure, generating the cryptographic components of the digital indicia, and securely adjusting the user registration. When a user wishes to print VBI , for example, postage or purchase additional VBI or postage value, a user state is instantiated in the PSD implemented within one of the cryptographic modules 110. Database 111 includes all the data accessible on-line for indicia creation, account maintenance, and revenue protection processes. Postage servers 109, Database 130, and cryptographic modules 110 are maintained in a physically secured environment, such as a vault.

FIG. 2 shows a simplified system block diagram of a typical Internet client/server environment used by an on-line VBI system in one embodiment of the present invention. PCs 220a-220n used by the postage purchasers are connected to the Internet 221 through the communication links 233a-233n. Each PC has access to one or more printers 235. Optionally, as is well understood in the art, a local network 234 may serve as the connection between some of the PCs, such as the PC 220a and the Internet 221 or other connections. Servers 222a-222m are also connected to the Internet 221 through respective communication links. Servers 222a-222m include information and databases accessible by PCs 220a-220n. The on-line VBI system of the present invention resides on one or more of Servers 222a-222m.

In this embodiment, each client system 220a-220m includes a CPU 223, a keyboard 224, a mouse 225, a mass storage device 231, main computer memory 227, video memory 228, a communication interface 232a, and an input/output device 226 coupled and interacting via a communication bus. The data and images to be displayed on the monitor 230 are transferred first from the video memory 228 to the video amplifier 229 and then to the monitor 230. The communication interface 232a communicates with the

servers 222a-222m via a network link 233a. The network link connects the client system to a local network 234. The local
5 network 234 communicates with the Internet 221.

In one embodiment, a customer (user), preferably licensed by the USPS and registered with an IBIP vendor (such as Stamps.com), sends a request for authorization to print a desired amount of VBI, such as postage. The server system verifies that
10 the user's account holds sufficient funds to cover the requested amount of postage, and if so, grants the request. The server then sends authorization to the client system. The client system then sends image information for printing of a postal indicium for the granted amount to a printer so that the postal indicium
15 is printed on an envelope or label.

In one embodiment, when a client system sends a VBI print request to the server system, the request needs to be authenticated before the client system is allowed to print the VBI, and while the VBI is being printed. The request is
20 cryptographically authenticated using an authentication code. The client system sends a password (or passphrase) entered by a user to the server for verification. If the password fails, a preferably asynchronous dynamic password verification method terminates the session and printing of the VBI is aborted. Also,
25 the server system communicates with a system located at a certification authority for verification and authentication purposes.

In one embodiment, the information processing components of the on-line VBI system include a client system, a postage server
30 system located in a highly secure facility, a USPS system and the Internet as the communication medium among those systems. The information processing equipment communicates over a secured communication line.

Preferably, the security and authenticity of the information
35 communicated among the systems are accomplished on a software

level through the built-in features of a Secured Socket Layer (SSL) Internet communication protocol. An encryption hardware
5 module embedded in the server system is also used to secure information as it is processed by the secure system and to ensure authenticity and legitimacy of requests made and granted.

The on-line VBI system is based on a client/server architecture. Generally, in a system based on client/server
10 architecture the server system delivers information to the client system. That is, the client system requests the services of a generally larger computer. In one embodiment, the client is a local personal computer and the server is a more powerful group of computers that house the information. The connection from the
15 client to the server is made via a Local Area Network, a phone line or a TCP/IP based WAN on the Internet or any other types of communication links such as wireless or satellite links. A primary reason to set up a client/server network is to allow many clients access to the same applications and files stored on the
20 server system.

The on-line VBI system does not require any special purpose hardware for the client system. The client system is implemented in the form of software that can be executed on a user computer (client system) allowing the user computer to function as a
25 virtual VBI meter. The software can only be executed for the purpose of printing the VBI indicia when the user computer is in communication with a server computer located, for example, at a VBI meter vendor's facility (server system). The server system is capable of communicating with one or more client systems
30 simultaneously.

In one embodiment, the on-line system includes the following subsystems: the Database subsystem, the Postal Server subsystem, the Provider Server subsystem, the E-commerce subsystem, the Staging subsystem, the Client Support subsystem, the Decision
35 Support subsystem, the SMTP subsystem, the Address Matching

service (AMS) subsystem, the SSL Proxy Server subsystem and the Web Server subsystem, and the like, as shown in FIG. 3.

5 Postage servers 109 in FIG. 1 include a string of servers connected to the Internet, for example, through a T1 line, and are preferably protected by a firewall. The firewall permits a client to communicate with a server system, only if the information packet transmitted by the client system complies with
 10 a security policy set by the server system. The services provided by the different subsystems of the on-line VBI system are designed to allow flexibility and expansion and reduce specific hardware dependency.

In one embodiment, the Database subsystem is comprised of
 15 multiple databases, as shown in FIG. 3. In this embodiment, the Database 411 includes the Affiliate DBMS and the Source IDs DBMS. The Affiliate DBMS manages affiliate information (e.g., affiliate's name, phone number, and affiliate's Website information) that is stored on the Affiliate Database. Using the
 20 data from this database, marketing and business reports are generated. The Source IDs Database contains information about the incoming links to the vendor's Website (e.g., partners' information, what services the vendor offers, what marketing program is associated with the incoming links, and co-branding
 25 information). Using the data from this database, marketing and business reports are generated.

The Online Store Database 412 contains commerce product information, working orders, billing information, password reset table, and other marketing related information. Website database
 30 410 keeps track of user accesses to the vendor website. This database keeps track of user who access the vendor website, users who are downloading information and programs, and the links from which users access the vendor website. After storing these data on the Website Database 410, software tools are used to generate
 35 the following information:

1 39478/RRT/S850

- Web Site Status
- Web Site Reports
- 5 • Form Results
- Download Successes
- Signup, Downloads, and Demographic Graphs
- Web Server Statistics (Analog)
- Web Server Statistics (Web Analyzer)

10 Offline database 409 manages the VBI data (except meter information), postal transactions data, financial transactions data (e.g., credit card purchases, free postage issued, bill credits, and bill debits), customer marketing information, commerce product information, meter license information, meter
15 resets, meter history, and meter movement information. Consolidation Server 413 acts as a repository for data, centralizing data for easy transportation outside the vault 400. The Consolidation Server hosts both file and database services, allowing both dumps of activity logs and reports as well as a
20 consolidation point for all database data.

The Offline Reporting Engine MineShare Server 415 performs extraction transformation from the holding database that received transaction data from the Consolidated Database (Commerce database 406, Membership database 408, and Postal Database 407).
25 Also, the Offline Reporting Engine MineShare Server handles some administrative tasks. Transaction data in the holding database contains the transaction information about meter licensing information, meter reset information, postage purchase transactions, and credit card transactions. After performing
30 extraction transformation, business logic data are stored on Offline Database 409. Transaction reports are generated using the data on the Offline Database. Transaction reports contain marketing and business information.

The Data Warehouse database 414 of FIG. 3 includes all
35 customer information, financial transactions, and aggregated

1 39478/RRT/S850

Postal Transaction Server 403 provides business logic for postal functions such as device authorization and postage
5 purchase/register manipulation. The Postal Transaction Server requires the cryptographic modules to perform all functions. There are four Client Support Servers. Address Matching Server (AMS) 417 verifies the correct address specified by a user. When the user enters a delivery address or a return address using the
10 Client Software, the user does not need the address matching database on the user's local machine to verify the accuracy of the address. The Client software connects to the vendor's server and uses the central address database obtained from the USPS to verify the accuracy of the address. If the address is incorrect,
15 the client software provides the user with a prioritized list of addresses to match the correct address. These choices are ranked in a user definable order. This information is represented using a plain text format.

The Client Support Servers 417 of FIG. 3 provides the
20 following services: a Pricing Plan service, an Auto Update service, and a Printer Config service. The Pricing Plan Service provides information on pricing plans and payment methods available to the user. It also provides what credit cards are supported and whether ACH is supported. This information is
25 represented preferably using a plain text format. The Auto Update Service verifies whether the user is running the latest Client Software. If there is newer Client Software, the Auto Update Server downloads the new patches to the user computer. The Client Support Database has tables for the client software
30 update information. This information is represented using a plain text format.

Before the user tries to print postage, the user sends his or her printer driver information over the Internet in plain text. The Printer Config Service looks up the printer driver
35 information in the Printer Driver Database to determine whether

1 39478/RRT/S850

the printer driver is supported or not. When the user tries to
configure the printer, the user prints a test envelope to test
5 whether the postage printing is working properly or not. This
testing envelope information is sent over the Internet in plain
text and is stored in the Client Support Database.

MeterGen server 422 makes calls into the cryptographic
module to create sufficient meters to ensure that the vendor can
10 meet customer acquisition demands. SMTP Server 418 communicates
with other SMTP servers, and it is used to forward e-mail to
users. Gatekeeper Server works as a proxy server by handling the
security and authentication validation for the smart card users
to access customer and administration information that reside in
15 the vault.

The Proxy Server 423 uses the Netscape™ Enterprise SSL
library to provide a secure connection to the vault 400. Audit
File Server 419 acts as a repository for module transaction logs.
The Audit File Server verifies the audit logs that are digitally
20 signed. The audit logs are verified in real time as they are
being created. Postal Server writes audit logs to a shared hard
drive on the Audit File Server. After these logs are verified,
the Audit File Server preferably moves them from the shared hard
drive to a hard drive that is not shared by any of the vendor
25 servers.

Provider Server provides reporting and external
communication functionality including the following services.
CMLS Service forwards license applications and it processes
responses from CMLS. The CMLS Service uses cryptographic
30 functions provided by the Stamps.com Crypt library to decrypt the
user's SSN/Tax ID/Employee ID. CMRS Service reports meter
movement and resetting to the USPS Computerized Meter Resetting
infrastructure. ACH Service is responsible for submitting ACH
postage purchase requests to the USPS lockbox account at the

35

1 39478/RRT/S850

bank. The CMLS Service uses cryptographic functions to decrypt the user's ACH account number.

5 After decrypting ACH account information, the ACH is encrypted using the vendor's script library. Then, the encrypted ACH file is e-mailed to the Commerce Group by the SMTP server. When the Commerce Group receives this encrypted e-mail, the vendor's Decrypt utility application is used to decrypt the ACH
10 e-mail. After verifying the ACH information, the Commerce Group sends the ACH information through an encrypted device first and then uses a modem to upload the ACH information to a proper bank. The Certificate Authority issues certificates for all IBIP meters. The certificates are basically used to provide
15 authentication for indicia produced by their respective meters.

The following are exemplary steps describing the certificate authorization process:

- MeterGen asks the module to create a meter package,
- The module returns a package and the meter's public key,
- 20 • MeterGen creates a certificate request with the public key, signs the request with a USPS-issued smartcard, and submits the request to the USPS Certificate Authority,
- The Certificate Authority verifies the request came from the vendor then, it creates a new certificate and returns it to MeterGen,
25
- MeterGen verifies the certificate using the USPS Certificate Authority's certificate (e.g., to ensure it wasn't forged) and stores the certificate information in the package. The package is now ready to be associated
30 with a customer.

The Postal Server subsystem 401 of FIG. 3 manages client and remote administration access to server functionality, authenticates clients and allows clients to establish a secure connection to the on-line VBI system. The Postal Server
35 subsystem also manages access to USPS specific data such as PSD

information and a user's license information. The Postal Server subsystem queries the Postal portion of the Database subsystem
 5 for the necessary information to complete the task. The query travels through the firewall to the Postal portion of the Database subsystem. The Postal Server subsystem is the subsystem in the Public Network that has access to the Database subsystem.

In one embodiment of the present invention, Postal Server
 10 401 is a standalone server process that provides secure connections to both the clients and the server administration utilities, providing both client authentication and connection management functionality to the system. Postal Server 401 also houses postal-specific services that require high levels of
 15 security, such as purchasing postage or printing indicia. Postal Server 401 is comprised of at least one server, and the number of servers increases when more clients need to be authenticated, are purchasing postage or are printing postage indicia.

If a user (customer) is using multiple PCs on one account,
 20 the user needs to re-register every time he/she switches computers. A Re-registration wizard helps the user through this process. The user-friendly re-registration process of the wizard does not require users to know their user IDs. An exemplary process flow diagram for a Re-registration wizard is depicted in
 25 FIG. 4.

Login screen 30 helps a user to login to the system. The client system sends the user name, password, and system identification information to the server system. After checking if the user name and password are valid (block 31), the server
 30 system then checks to determine if the user is currently registered on the current system, or on another one, as shown in block 32. If the user is registered on the current system (computer), login continues as normal, as shown in block 33. If the user is currently registered on another system, the user sees
 35 a screen that takes the user into the Re-registration wizard.

1 39478/RRT/S850

If the account is currently logged in, a re-registration screen is shown (block 36) and if the account is in use the login process is canceled, as shown in block 37. If the account is not currently logged in, a registration screen (block 38) asks the user whether he wants to re-register (block 39). If the user decides to not register, the login process is canceled, as shown in block 41.

10 The system determines the specific systems or PCs that users used by storing information specific to those systems (PCs). In one embodiment, the system-specific information includes register settings, processor's unique ID, machine configuration, network card ID, a user's private key, and the like.

15 In one embodiment, the system uses a hash message authentication (HMK) key to identify the specific computer (machine) that a user had used to use the system. The client software randomly generates the HMK at the time of user registration. This HMK key is encrypted using a 3DES key derived from the user passphrase. The key is stored on the user's computer before it is sent to the Postal Server during the registration stage. This key is changed on a regular basis. The cryptographic module that resides inside the Postal Server stores this HMK key in a secure database after encryption as a part of the user's PSD package. All cryptographic modules have access to the HMK keys that are stored in this secure database.

20 The cryptographic module public key that is used to encrypt the user HMK during the key sharing stage is embedded inside the client software package. The cryptographic module uses its corresponding private key to decrypt the encrypted user HMK forwarded by the Postal server during the user registration stage. This security technique is generally more difficult to break than simply using a user's password as a security method. The encrypted HMK key on the user's computer is decrypted when a user logs on to the client software with the proper password.

screen in the Re-registration wizard opens. If the user clicks "No", the Cancel Re-Registration Failed Screen opens.

5 The exemplary Name and Password screen of FIG. 5C is the first substantive screen of the Re-registration wizard. This screen lets the user enter his/her user name and password. This screen can be accessed by checking the "I have already registered with Stamps.com" check box on the Welcome Screen of a Getting
10 Started Wizard. Alternatively, it can be accessed from the vendor Program Group - vendor Internet Postage Re-register. Finally, this screen opens if the user clicks "Yes" in the "Account is Registered on Another Computer" screen. Preferably, the "Cancel" and "Help" buttons are enabled on open. The "Next>"
15 button becomes enabled when the user has entered text into both fields. Preferably, the "<Back" button is not enabled.

The "Secret Code Response" screen show in FIG. 5D allows the user to enter the secret code they supplied when they first registered with a vendor. Preferably, the question changes based
20 on the original secret code question selected by the user. For example, if the user selected "Pet's name" the question reads, "What is your favorite pet's name?" Preferably, if the user entered an incorrect user name or password in the previous screen, this screen opens with the "Mother's maiden name"
25 question. This helps guard against fraud. Preferably, the "<Back", "Cancel" and "Help" buttons are enabled on open. The "Next>" button becomes enabled when the user has entered text into both field. If the user entered the correct information in both screens, the exemplary screen of FIG. 5E opens to tell the
30 user that re-registration was successful. If the user clicks the "Cancel" button at any time during the re-registration process, the exemplary screen shown in FIG. 5F opens.

FIGs. 5G-5I are exemplary error screens for the Re-registration wizard. The Password-Length screen of FIG. 5G opens
35 if the password is for example, less than 6 or greater than 14

characters. The "No Number in Password" screen of FIG. 5H opens if the password does not contain any numbers. The No-Alphabetic-Character-in-Password screen of FIG. 5I opens if the password does not contain any letters. A "Secret Code Response Error" screen opens after the "Secret Code Response" screen. This screen will also open if there are errors in either the "Secret Code Response" or "User Name and Password" screens.

10 If the user enters incorrect information in either or both screens the exemplary screen shown in FIG. 5J opens. Preferably, the user is not told which information is incorrect to protect against fraud. Preferably, the "Cancel" and "Help" buttons are enabled on open. The "Next>" button becomes enabled when the user has entered text into both fields. Preferably, the "<Back" button is not enabled. Typically, some users lose their passwords and will not be able to login to the system. Giving anyone but the user access to their password would be a major security violation. The following describe a process for user password recovery.

20 The password recovery process maintains a high level of security, while still allowing a user the flexibility to gain access to the client software. In the current systems, Customer Support (CS) verifies user identity based on the last four digits of the user's Social Security #. This presents two problems: 1) not all users will input their SSN, they have the option to input Employer ID or Tax ID 2) most personal information (name, social security/tax id number, e-mail address, etc.) can be stolen or discovered easily by a third party.

30 To overcome these problems, the system uses a "code word" for user verification. This word is recorded during registration, and is something natural to the user. During registration, the users will be given the choice of a few different types of code word associated with a question (e.g., what is your mother's maiden name?). If a Customer Support Representative (CSR) needs

1 39478/RRT/S850

incorrect information 5 times in a row, she should close and reopen the client or contact Customer Service.

- 5 • Did the user enter the information correctly by the 5th time? Go to step 3
- Did the user fail to enter information correctly by the 5th time and closed and re-opened the client? Repeat step 2
- 10 • Did the user fail to enter information correctly by the 5th time and contacted Customer Service via e-mail? Go to step 9
- Did the user fail to enter information correctly by the 5th time? Contact Customer Service via phone, go to step 4
- 15 • Dialog states "Your temporary Resetting Password was sent to xxx@xxxx.net, please return to this screen to enter your temporary password". Go to step 7
4. User calls Customer Support to reset password
- User tells CSR they forgot their password. Go to step 5
- 20 5. CSR goes to PW Recovery screen
- CSR asks user validation questions.
- CSR enters responses (code word + last 4 digits of SSN or Tax ID or EID) in dialog - does not have viewing rights to information. CSR reads answers back to user for verification.
- 25 • Did the CSR enter information correctly? Go to step 6
- Did the CSR fail to enter information correctly by the 5th time? Close and re-open the Password Recovery screen. Repeat step 5
- 30 6. The user is automatically e-mailed a password good for one login.
- The Postal Servers randomly generates the password send the e-mail.
- CSR receives confirmation was e-mailed, is shown the e-mail address where e-mail was sent.
- 35

1 39478/RRT/S850

- Go to step 8
- 7. User logs into client with temporary password
- 5 • Client dialog box forces user to enter a new permanent password
- User cannot access any client features until a new password is entered
- 8. END
- 10 9. CSR receives e-mail
- CSR should look up user in CS interface with info that is on their e-mail. They access the Password Recovery screen to find the code word question, just as if the user was on the phone
- 15 10. CSR replies to user
- CSR uses standard internal (non-Postal System) e-mail form to ask for SSN or Tax ID or EID + code word question. Go to step 11
- 11. User replies to CS e-mail
- 20 • CSR enters information into Password Recovery screen. If the user's response is not valid, the CSR send the user an e-mail asking them to resubmit. If it is valid, the CSR hits "OK" at the e-mail prompt. Go to step 6.
- FIGs. 7A-7G are exemplary screens for supplying a secret code and password recovery. In one embodiment, the screens asking for Secret Code may be integrated with the client Registration wizard. The "Lost Password" option may be added to the existing Log-In dialog. Lost Password screens may be required as additional dialog within the client. FIG. 7A is an exemplary screen for supplying a secret code. In one embodiment, the screen fits into the Registration wizard and preferably has the following functionality:
- None of the code word types are selected by default
- The "Next>" button is disabled until the user selects a Secret Code type and enters a valid Secret Code
- 35

1 39478/RRT/S850

number. Once they are entered, the CSR has no other access to this information.

5 Once the CSR successfully enters the code word and identification number, the CSR is prompted to confirm the user's current e-mail address and change it if necessary. The user is then sent an e-mail with a new, randomly generated password. The CSR is shown a message to this effect and will inform the user.
10 A sample Password Recovery screen is shown in FIG. 8A. In this screen:

- <mother's maiden name> will be dynamically replaced with the appropriate Secret Word type question
- <Tax Identification Number> will be replaced with the
15 appropriate identification number question
- Contact via Phone radio button is default value

If the CSR enters the information incorrectly, the dialog box shown in FIG. 8B opens. The "OK" button in this dialog box returns the CSR to the PW screen. Once the CSR successfully
20 enters the information, they need to confirm the user's e-mail address or give the user the option to receive the password via mail. The message: of FIG. 8C then appears. In this dialog box, the "OK" button closes the password recovery screen. If the user never receives the auto e-mail, the user should again call
25 CS to repeat the process to have a new one generated.

For the situations where a person initiates a password reset via e-mail, the standard e-mail template that Customer Support uses to ask that person for their code and identification number should also include instructions on how to reset their password
30 via the client. An example of this e-mail appears below. The CS Manager should be able to alter the text through standard operational procedures and QA. The CSR will obtain the correct word question and identification number type from the normal CSR Password Recovery screen (which is populated based on the user's
35 profile).

1 39478/RRT/S850

Dear <customer>,

5 *In order to complete your request, you will need to answer the following questions:*

- *What is your <mother's maiden name>?*
- *What are the last four digits of your <social security number>?*

10 *Once we have received and verified your answers, we will e-mail you a temporary password.*

15 A Password Reset Activity report can be generated by the system. This activity report is a summary that shows all the password reset activity for a time period. This report is not time-critical and can be generated from the offline database. A Password Reset Activity report may also be generated by the system. This report is a summary report of all password reset and related activities generated from the Offline database.

20 A Customer Profile database in the server system includes the following fields to support the temporary password reset process:

- A Secret Word field (suggested type and length is varchar - 30)
- A Secret Word type field.
- A code field (suggested type is code integer) that identifies if the password was reset through the client; by Customer Support via e-mail; or Customer Support via phone.
- Last four digits of user's Identification number, taken during Registration
- Code (or full description) for the Identification number, classifying it as a SSN, Employer ID or Tax ID.

30 Since the code word and code word types are personal identification information, they are preferably stored in the same table and with the same level of security as other personal user information.

35 The postal servers compare Resetting password information

1 39478/RRT/S850

during the installation process. The option of the "silent
install" installs the program files to the user's system without
5 being visible, and without requiring user intervention.

For the default directory path option, the installer needs
to be told where to install the product's files. While the user
may choose to install the product in any directory location they
want, the installer offers them a choice consistent with the
10 product identity. Every product is placed in a sub-directory
within the master directory. The OEM partner or the advertiser
has the ability to provide a name for both the master directory
and sub-directory into which the Internet VBI product will be
installed.

15 For the default installation group choice, the program
group, or "folder", is the location in which the installer will
display the product if the user does not manually choose a
different one. The system allows the OEM partner or the
advertiser to customize the Default Program Group name. The OEM
20 partner or the advertiser does not have the ability, however, to
change the name or associated icons of the items within the
group.

In the case of a postal indicium, the system provides a
space within the postal indicium that is designated to display
25 a logo or slogan of the OEM partner or the advertiser, as shown
in FIG. 9. The graphic image provided by the OEM partner or the
advertiser may be saved in any graphics formats such as Windows
Bitmap (BMP), GIF, JPEG, or other graphic formats.

The client server technology of the Internet VBI system
30 enables a provider to provide OEM partners and advertisers with
data that tracks the VBI usage of users who are using that OEM's
version of the client software. The system embeds a unique OEM
identifier within each OEM version of the client software. Once
a user has registered with a provider, that user is thereafter
35 associated with the OEM that is identified within their client

1 39478/RRT/S850

have just passed the threshold period during the previous
month, which ensures that a user will only appear on this
5 report once.

It will be recognized by those skilled in the art that
various modifications may be made to the illustrated and other
embodiments of the invention described above, without departing
from the broad inventive scope thereof. It will be understood
10 therefore that the invention is not limited to the particular
embodiments or arrangements disclosed, but is rather intended to
cover any changes, adaptations or modifications which are within
the scope and spirit of the invention as defined by the appended
claims.

15

20

25

30

35

1 39478/RRT/S850

WHAT IS CLAIMED IS:

5 1. An on-line system for printing a value bearing item (VBI) comprising:

a user using one or more computers connected to a computer network;

a secret key for identifying a first computer used by the user for registering with the on-line system;

10 a server system capable of communicating with the one or more user computers over the computer network for receiving user information and the secret key from the first computer and registering a user; and

15 a re-registration wizard for requiring the user to re-register if a second computer used by the user is not the same as the first computer used for registering the user.

20 2. The system of claim 1, further comprising one or more client software resident on the one or more user computers, wherein each client software include a graphical user interface (GUI).

25 3. The system of claim 1, wherein the secret key comprises a hash message authentication key (HMK).

4. The system of claim 3, wherein the HMK is randomly generated in a user computer at the time of user registration with the on-line system.

30 5. The system of claim 3, wherein the HMK is encrypted.

6. The system of claim 3, wherein the HMK is encrypted using a Triple DES key derived from a user passphrase.

35

1 39478/RRT/S850

7. The system of claim 3, wherein the HMK is used to sign individual server requests and authenticate the user for each server request.

8. The system of claim 3, wherein the HMK is stored at the user computer.

9. The system of claim 3, wherein the HMK is changed on a periodic basis.

10. The system of claim 1, wherein the server system includes a cryptographic module for storing the secret key in a secure database.

11. The system of claim 1, wherein the secret key is stored as a part of a user PSD package.

12. The system of claim 10, wherein the cryptographic module uses a corresponding private key to decrypt encrypted secret keys.

13. The system of claim 1, wherein the VBI bears postage value.

14. The system of claim 1, wherein the VBI is a ticket.

15. The system of claim 1, wherein the VBI is one or more of a coupon, a currency, a voucher, and a check.

16. A method for printing a value bearing item (VBI) by a user using one or more computers connected to a computer network, the method comprising the steps of:

registering by the user with an on-line system for

1 39478/RRT/S850

printing a(VBI)

generating a secret key for identifying a first
5 computer used by the user for registering with the on-line
system;

receiving user information and the secret key from the
first computer by a server system capable of communicating with
the one or more user computers over the computer network;

10 identifying a second computer used by the user to logon
to the on-line system using the secret key; and

requiring the user to re-register if the second
computer used by the user is not the same as the first computer
used for registering the user.

15 17. The method of claim 16, wherein the secret key
comprises a hash message authentication key (HMK).

18. The method of claim 17, further comprising the step of
20 randomly generating the HMK in a user computer at the time of
user registration with the on-line system.

19. The method of claim 17, further comprising the step of
encrypting the HMK.

25 20. The method of claim 17, further comprising the step of
encrypting the HMK using a Triple DES key derived from a user
passphrase.

30 21. The method of claim 17, further comprising the step of
using the HMK to sign individual server requests and authenticate
the user for each server request.

22. The method of claim 17, further comprising the step of
35 storing the HMK at the user computer.

23. The method of claim 17, further comprising the step of changing the HMK on a periodic basis.

5

24. The system of claim 16, further comprising the step of storing the secret key in a secure database remote from the user computer.

10

25. The method of claim 16, further comprising the step of storing the secret key as a part of a user PSD package.

15

26. The method of claim 16, wherein the step of printing the VBI comprises printing a postage value.

27. The method of claim 16, wherein the step of printing the VBI comprises printing a ticket.

20

28. The method of claim 16, wherein the step of printing the VBI comprises printing one or more of a coupon, a currency, a voucher, and a check.

29. An on-line system for printing a value bearing item (VBI) comprising:

25

a user using one or more computers connected to a computer network;

a memory for storing information specific to a first computer used by the user for registering with the on-line system, wherein the information is used by the server system to identify the first computer;

30

a server system capable of communicating with the one or more user computers over the computer network for receiving user information and the computer information from the first computer; and

35

a re-registration wizard for requiring the user to re-

1 39478/RRT/S850

register if a second computer used by the user is not the same as the first computer used for registering the user.

5

30. The system of claim 29, wherein the information specific to a first computer include one or more of register settings, a processor's ID, machine configuration, a network card ID, and a user's private key.

10

31. The system of claim 29, wherein the information specific to a first computer is encrypted.

32. The system of claim 29, wherein the information specific to a first computer is encrypted using a Triple DES key derived from a user passphrase.

15

33. The system of claim 29, wherein the server system includes a cryptographic module for storing the information specific to a first computer in a secure database.

20

34. The system of claim 29, wherein the VBI bears postage value.

35. The system of claim 29, wherein the VBI is a ticket.

25

36. The system of claim 29, wherein the VBI is one or more of a coupon, a currency, a voucher, and a check.

37. A method for printing a value bearing item (VBI) by a user using one or more computers connected to a computer network, the method comprising the steps of:

30

registering by the user with an on-line system for printing a(VBI)

storing information specific to a first computer used

35

1 39478/RRT/S850

by the user for registering with the on-line system, wherein the
information is used by the server system to identify the first
5 computer;

receiving user information and the information specific
to the first computer from the first computer by a server system;

identifying a second computer used by the user to logon
to the on-line system using the information specific to the
10 second computer; and

requiring the user to re-register if the second
computer used by the user is not the same as the first computer
used for registering the user.

15 38. The method of claim 37, wherein the information
specific to a first computer include one or more of register
settings, a processor's ID, machine configuration, a network card
ID, and a user's private key.

20 39. The method of claim 37, further comprising the step of
encrypting the information specific to a first computer.

40. The method of claim 37, further comprising the step of
encrypting the information specific to a first computer using a
25 Triple DES key derived from a user passphrase.

41. The method of claim 37, further comprising the step of
storing the information specific to a first computer at the user
computer.

30 42. The system of claim 37, further comprising the step of
storing the information specific to a first computer in a secure
database remote from the user computer.

35

1 39478/RRT/S850

43. The method of claim 37, wherein the step of printing the VBI comprises printing a postage value.

5

44. The method of claim 37, wherein the step of printing the VBI comprises printing a ticket.

45. The method of claim 37, wherein the step of printing the VBI comprises printing one or more of a coupon, a currency, a voucher, and a check.

15

20

25

30

35

1 39478/RRT/S850

MACHINE DEPENDENT LOGIN FOR ON-LINE
VALUE-BEARING ITEM SYSTEM

5

ABSTRACT OF THE DISCLOSURE

An on-line VBI printing system that includes one or more cryptographic modules and a central database. The cryptographic modules are capable of implementing a variety of required security standards. A client system provides a user friendly GUI for facilitating the interface of the user to the system. The GUI system includes wizards that help the user step-by-step with processes of registration, logging into the system, and printing the VBI.

15 In one aspect, the invention describes an on-line system for printing a value bearing item (VBI) that includes a memory for storing information specific to a first computer used by the user for registering with the on-line system, wherein the information is used by the server system to identify the first computer and a re-registration wizard for requiring the user to re-register if a second computer used by the user is not the same as the first computer used for registering the user.

25

RRT/dz

DSZ PAS280575.1--*-10/18/00 2:21 PM

30

35

FIG. 1

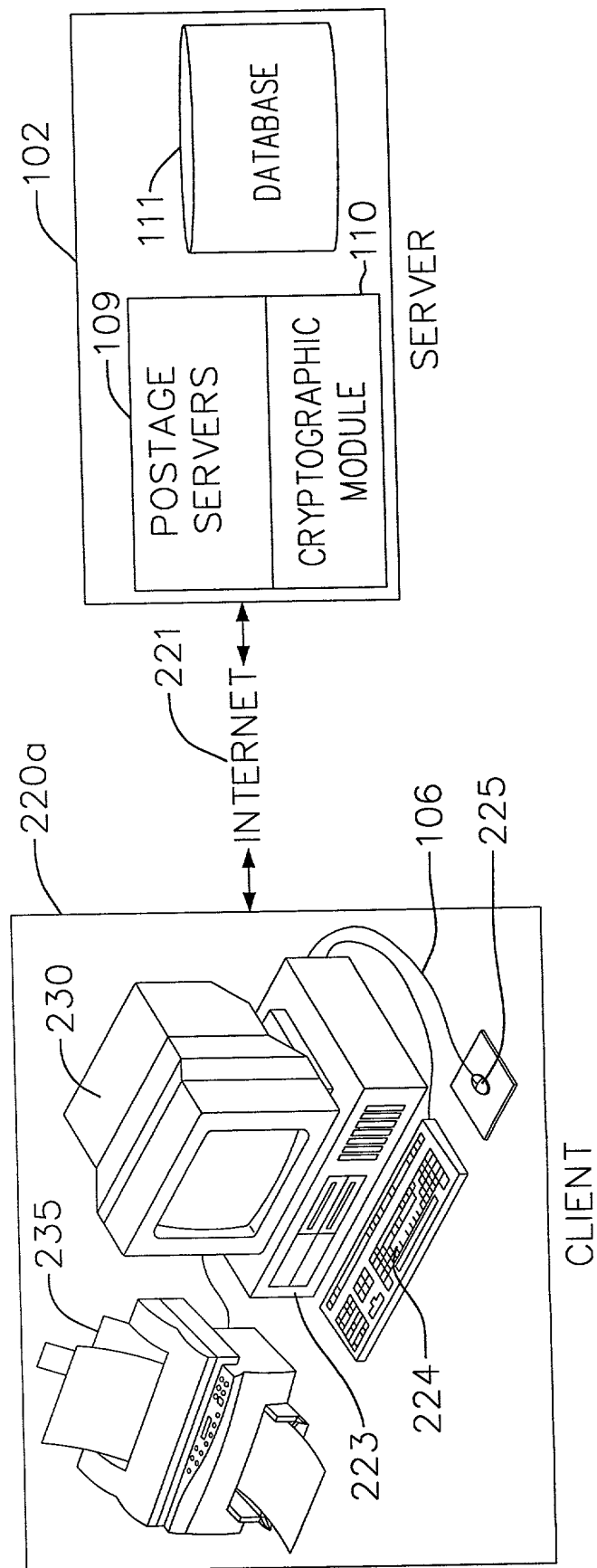
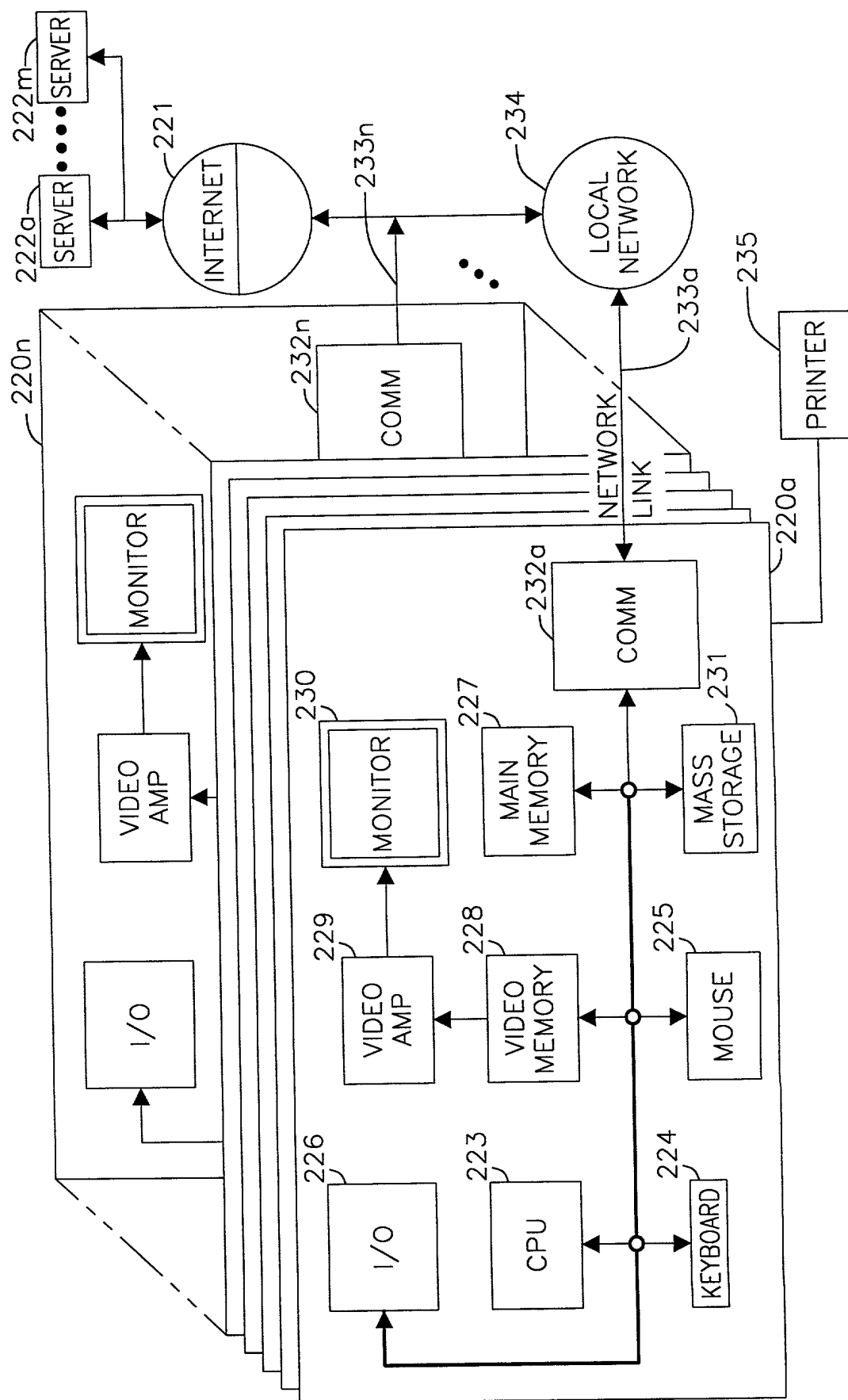
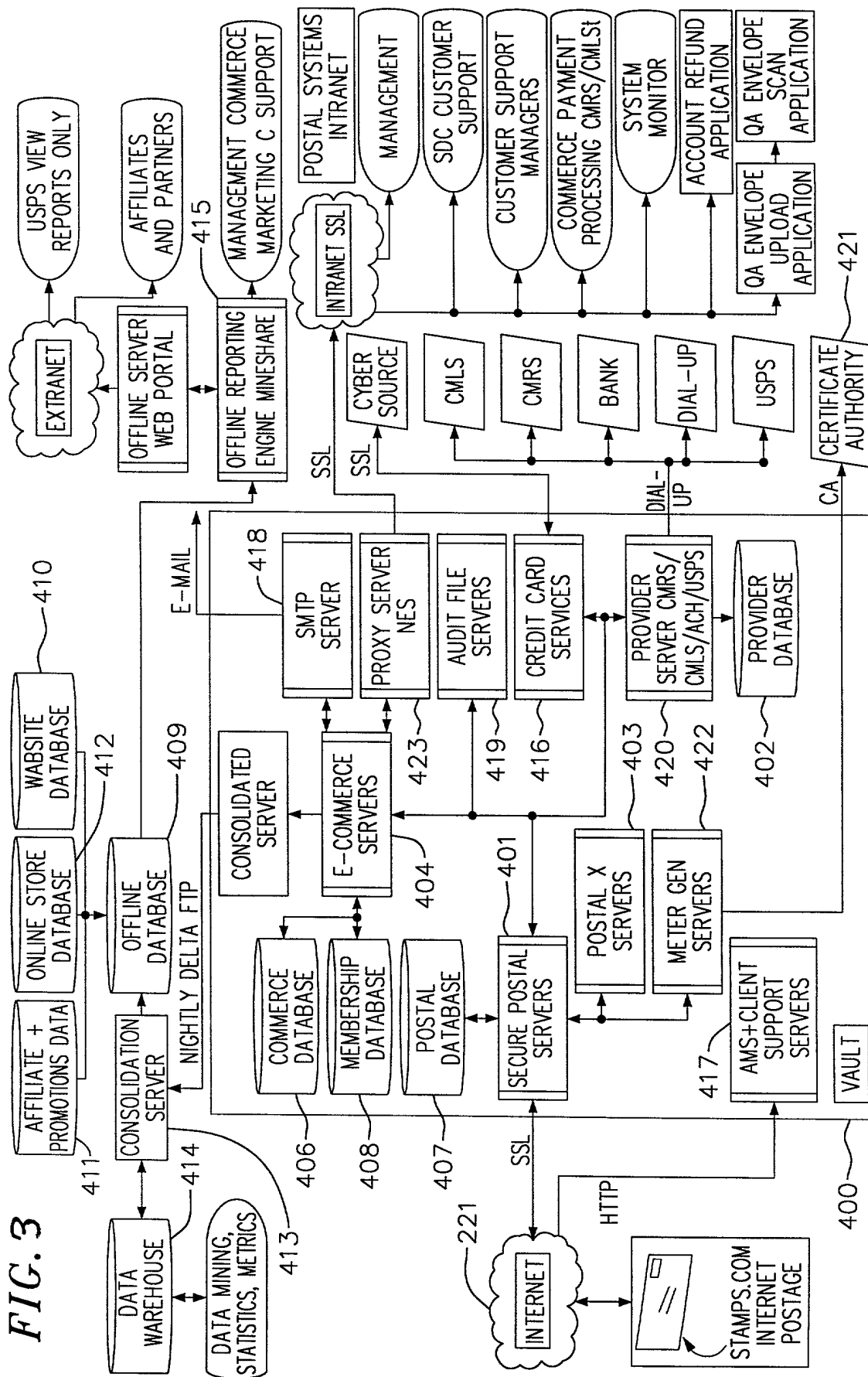


FIG. 2





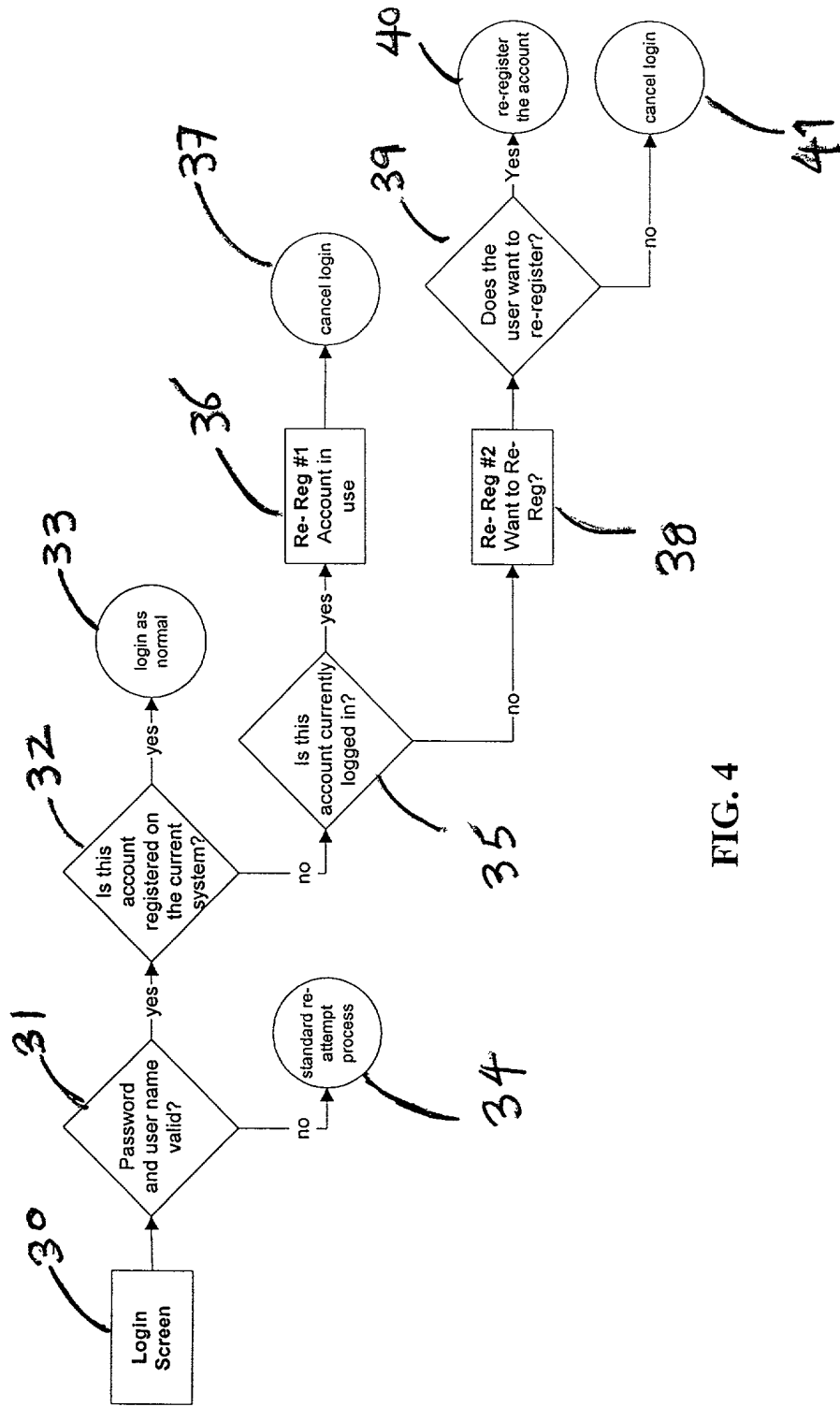


FIG. 4

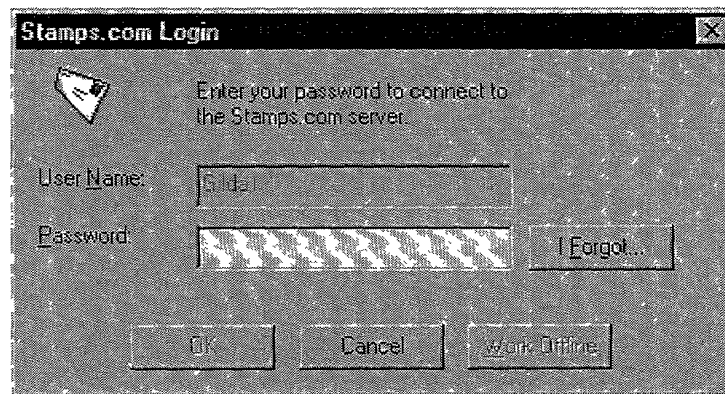


FIG. 5A

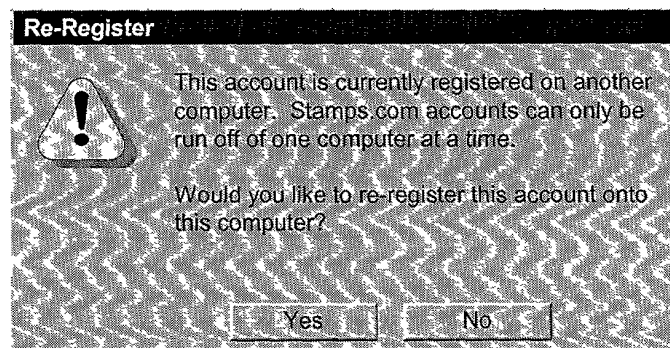


FIG. 5B

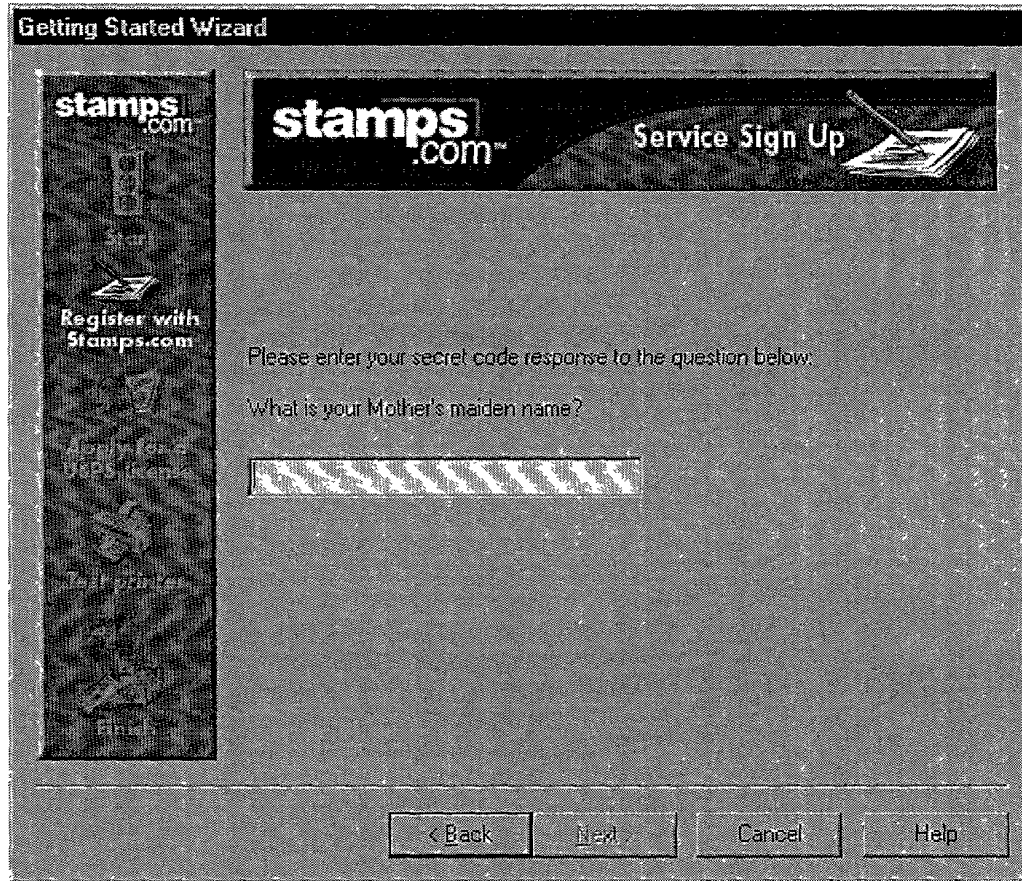


FIG. 5D



FIG. 5E

FIG. 5F



FIG. 5G



FIG. 5H

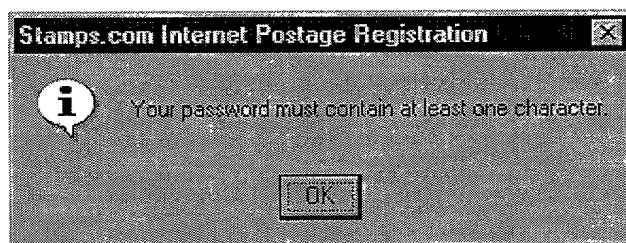


FIG. 5I

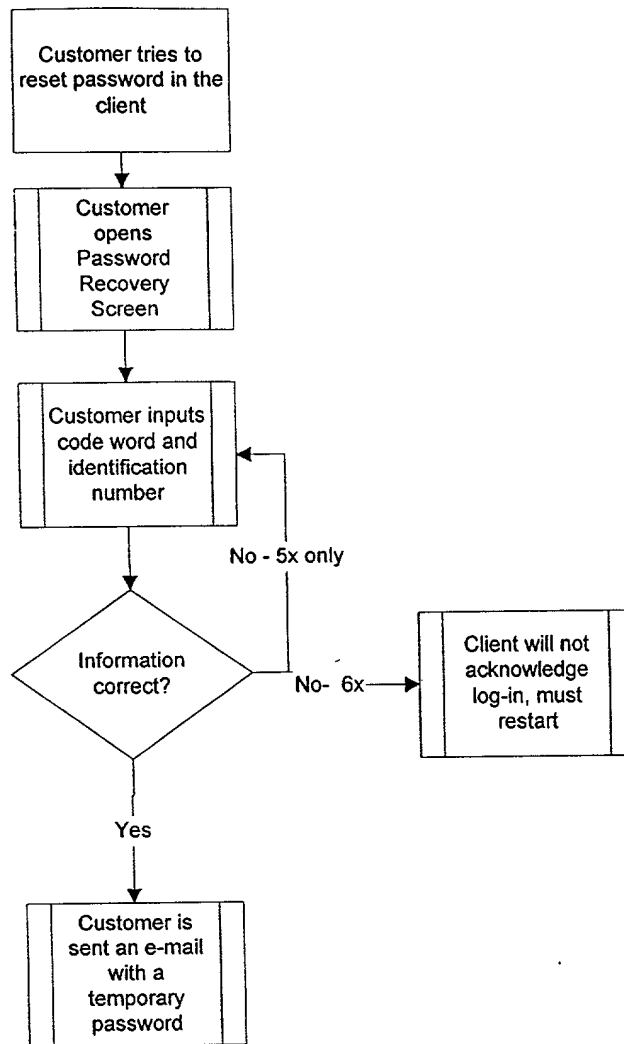


FIG. 6A

```

graph TD
    A[Customer calls Customer Support to reset password] --> B[CSR opens Password Recovery Screen]
    B --> C[CSR asks customer their code word question, user name, and identification number]
    C --> D{Customer answers questions correctly?}
    D -- No --> C
    D -- Yes --> E[Customer is sent an e-mail with a temporary password]
  
```

FIG. 6B

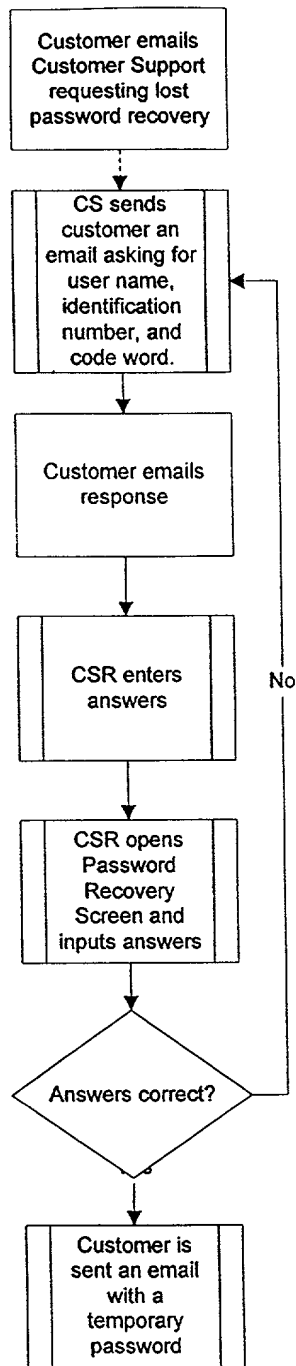


FIG. 6C

Stamps.com Internet Postage

Please enter your temporary password and the new password you have selected.

Temporary Password:

New Password:

Confirm New Password:

FIG. 7D

Password Recovery

Please answer the following questions:

What is your <mother's maiden name>?

What are the last four digits of your <Tax Identification Number>?

FIG. 7E

Stamps.com Internet Postage



 The information you entered was incorrect.
Please try again.

FIG. 7F



Confirmation

Your entry has been confirmed! A temporary password has been sent to <blahblah@bleh.com>. You must exit and log back in to use this new password.

OK

FIG. 7G

NAME	USER NAME	USER ID	METER #
Dow, John	Johnny	38745942	3458250333

Password Recovery

Enter the customer's code word and last 4 digits of the identification number


What is your <mother's maiden name>?

What are the last 4 digits of your
<Employee Identification Number>?

The customer contacted you by:

☒ Phone ☐ Email

FIG. 8A

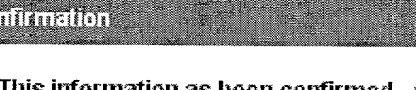


Error

The information entered was incorrect.
Please try again.

OK

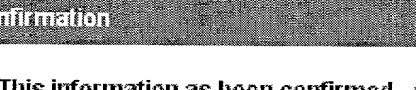
FIG. 8B

A screenshot of a confirmation dialog box. The title bar at the top is dark gray with the word "Confirmation" in white. The main area is white and contains the text: "This information as been confirmed. A temporary password has been sent to this customer at <blahblah@bleh.com>". At the bottom center is a button with a light gray background and the text "OK" in black.

Confirmation

This information as been confirmed. A temporary password has been sent to this customer at <blahblah@bleh.com>

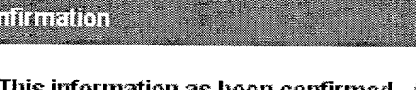
OK

A screenshot of a confirmation dialog box. The title bar at the top is dark gray with the word "Confirmation" in white. The main area is white and contains the text: "This information as been confirmed. A temporary password has been sent to this customer at <blahblah@bleh.com>". At the bottom center is a button with a light gray background and the text "OK" in black.

Confirmation

This information as been confirmed. A temporary password has been sent to this customer at <blahblah@bleh.com>

OK

A screenshot of a confirmation dialog box. The title bar at the top is dark gray with the word "Confirmation" in white. The main area is white and contains the text "This information as been confirmed. A temporary password has been sent to this customer at <blahblah@bleh.com>". At the bottom center is a button with a light gray background and the text "OK" in black.

Confirmation

This information as been confirmed. A temporary password has been sent to this customer at <blahblah@bleh.com>

OK

FIG. 8C

[illegible]

**DECLARATION AND POWER OF ATTORNEY
FOR PATENT APPLICATIONS**

PATENT

Docket No. : 39478/RRT/S850

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled MACHINE DEPENDENT LOGIN FOR ON-LINE VALUE-BEARING ITEM SYSTEM, the specification of which is attached hereto unless the following is checked:

___ was filed on ___ as United States Application Number or PCT International Application Number ___ and was amended on ___ (if applicable).

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR § 1.56.

I hereby claim foreign priority benefits under 35 U.S.C. § 119(a)-(d) or § 365(b) of the foreign application(s) for patent or inventor's certificate, or § 365(a) of any PCT International application which designated at least one country other than the United States, listed below and have also identified below, any foreign application for patent or inventor's certificate, or PCT International application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application(s)

<u>Application Number</u>	<u>Country</u>	<u>Filing Date (day/month/year)</u>	<u>Priority Claimed</u>
---------------------------	----------------	-------------------------------------	-------------------------

I hereby claim the benefit under 35 U.S.C. § 119(e) of any United States provisional application(s) listed below.

<u>Application Number</u>	<u>Filing Date</u>
60/160,040	October 18, 1999
60/160,038	October 18, 1999
60/160,491	October 20, 1999
60/160,708	October 20, 1999

I hereby claim the benefit under 35 U.S.C. § 120 of any United States application(s), or any PCT International application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of 35 U.S.C. § 112, I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR § 1.56 which became available between the filing date of the prior application and the national or PCT International filing date of this application:

<u>Application Number</u>	<u>Filing Date</u>	<u>Patented/Pending/Abandoned</u>
---------------------------	--------------------	-----------------------------------

POWER OF ATTORNEY: I hereby appoint the following attorneys and agents of the law firm CHRISTIE, PARKER & HALE, LLP to prosecute this application and any international application under the Patent Cooperation Treaty based on it and to transact all business in the U.S. Patent and Trademark Office connected

**DECLARATION AND POWER OF ATTORNEY
FOR PATENT APPLICATIONS**

Docket No. 39478/RRT/S850

with either of them in accordance with instructions from the assignee of the entire interest in this application; or from the first or sole inventor named below in the event the application is not assigned; or from __ in the event the power granted herein is for an application filed on behalf of a foreign attorney or agent.

R. W. Johnston	(17,968)	Gregory S. Lampert	(35,581)	Cynthia A. Bonner	(44,548)
D. Bruce Prout	(20,958)	Grant T. Langton	(39,739)	Jun-Young E. Jeon	(43,693)
Hayden A. Carney	(22,653)	Constantine Marantidis	(39,759)	Marc A. Karish	(44,816)
Richard J. Ward, Jr.	(24,187)	Daniel R. Kimbell	(34,849)	John F. O'Rourke	(38,985)
Russell R. Palmer, Jr.	(22,994)	Craig A. Gelfound	(41,032)	Richard J. Paciulan	(28,248)
LeRoy T. Rahn	(20,356)	Syed A. Hasan	(41,057)	Josephine E. Chang	(46,083)
Richard D. Seibel	(22,134)	Kathleen M. Olster	(42,052)	Frank L. Cire	(42,419)
Walter G. Maxwell	(25,355)	Daniel M. Cavanagh	(41,661)	Harold E. Wurst	(22,183)
William P. Christie	(29,371)	Molly A. Holman	(40,022)	Robert A. Green	(28,301)
David A. Dillard	(30,831)	Lucinda G. Auciello	(42,270)	Derrick W. Reed	(40,138)
Thomas J. Daly	(32,213)	Norman E. Carte	(30,455)	John W. Peck	(44,284)
Vincent G. Gioia	(19,959)	Joel A. Kauth	(41,886)	Stephen D. Burbach	(40,285)
Edward R. Schwartz	(31,135)	Patrick Y. Ikehara	(42,681)	David B. Sandelands, Jr.	(46,023)
John D. Carpenter	(34,133)	Mark Garscia	(31,953)	Heidi L. Eisenhut	(46,812)
David A. Plumley	(37,208)	Gary J. Nelson	(44,257)	Nicholas J. Pauley	(44,999)
Wesley W. Monroe	(39,778)	Raymond R. Tabandeh	(43,945)	Mark J. Marcelli	(36,593)

The authority under this Power of Attorney of each person named above shall automatically terminate and be revoked upon such person ceasing to be a member or associate of or of counsel to that law firm.

DIRECT TELEPHONE CALLS TO : Raymond R. Tabandeh, 626/795-9900

**SEND CORRESPONDENCE TO : CHRISTIE, PARKER & HALE, LLP
P.O. Box 7068, Pasadena, CA 91109-7068**

I declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full name of sole or first joint inventor Craig L. Ogg	Inventor's signature	Date
Residence and Post Office Address Long Beach, California		Citizenship U.S.

Full name of second joint inventor Piers C. Lingle	Inventor's signature	Date
Residence and Post Office Address Santa Monica, California		Citizenship U.S.